

Complex Hadamard matrices for prime numbers

Petre Diță*

Horia Hulubei National Institute of Physics and Nuclear Engineering, P.O. Box MG6, Magurele, Romania

In this paper we disprove the Haagerup statement that all complex Hadamard matrices of order five are equivalent with the Fourier matrix F_5 by constructing circulant matrices that lead to new Hadamard matrices. An important item is the construction of new mutually unbiased bases that are a basic concept of quantum theory and play an essential role in quantum tomography, quantum cryptography, teleportation, construction of dense coding schemes, classical signal processing, etc.

1. INTRODUCTION

Björck G. and Fröberg R., [1], seem to be the first authors who treated the problem of cyclic n -roots with applications to Hadamard matrices.

T. Durt and his coworkers, [2], studied the classification problem of Hadamard matrices of size $n \leq 5$. In particular they used the *dephased* form for all matrices. They says that the (rescaled) Fourier matrices are the unique example in order $n \leq 3$, and in order 5 one has uniqueness again, result which already is absolutely non-trivial! Their example for $n = 3$ is the following

$$F_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma \end{bmatrix} \quad (1)$$

where $\gamma = e^{\frac{2\pi i}{3}}$, citing the paper [1].

Because this approach is spreading fast, see paper [4], we construct many three and five dimensional Hadamard matrices that disprove the Szöllősi assumption that only the Fourier matrices F_3 and F_5 have a real existence. Szöllősi in his thesis, [3], seems to agree that a complete classification of complex Hadamard matrices is only available up to order $n = 5$, and in this case it is equivalent with the Fourier matrix F_5 .

In this paper we consider the cases $n = 2$, $n = 3$ and $n = 5$.

The orthogonality concept is essential for getting new complex Hadamard matrices and in the following we make use of the particular class of inverse orthogonal matrices, $O = (o_{ij})$, whose inverse is given by

$$O^{-1} = (1/o_{ij}^t) = (1/o_{ji}) \quad (2)$$

where t means transpose, and their entries, $0 \neq o_{ij} \in \mathbb{C}$, satisfy the relation

$$OO^{-1} = nI_n \quad (3)$$

When o_{ij} entries take unimodular values, O^{-1} coincides with the Hermitean conjugate O^* of O , and in this case O/\sqrt{n} is the definition of complex Hadamard matrices, see for example paper [5].

2. THE TWO DIMENSIONAL CASE

We start with the simplest case $n = 2$ and we use the next matrix in order to find new Hadamard matrices

$$C_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (4)$$

*Electronic address: dita@zeus.theory.nipne.ro

This matrix is not Hadamard. Thus we make use of the relation (3) which provides the following constraint $bc + ad = 0$. By using it we find four solutions

$$H_1 = \begin{bmatrix} \frac{bc}{d} & b \\ c & d \end{bmatrix}, H_2 = \begin{bmatrix} a & -\frac{ad}{c} \\ c & d \end{bmatrix}, H_3 = \begin{bmatrix} a & b \\ -\frac{bc}{a} & d \end{bmatrix}, H_4 = \begin{bmatrix} a & b \\ c & -\frac{bc}{a} \end{bmatrix} \quad (5)$$

The above matrices generate many MUBs (\mathbb{I}, H_1, H_2) , (\mathbb{I}, H_1, H_3) , (\mathbb{I}, H_2, H_4) , etc.

3. THE THREE DIMENSIONAL CASE

As usual we make use of the Sylvester orthogonality, see paper [5], and we start with the circulant matrix C_3 whose form is

$$C_3 = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \quad (6)$$

and C_3 matrix provides the following parameter constraints

$$a^2b + b^2c + ac^2 = 0, ab^2 + a^2c + bc^2 = 0 \quad (7)$$

When they are satisfied C_3 transforms into new matrices which are not yet Hadamard. For example from the first equation (6) one gets

$$a = \frac{-c^2 \pm \sqrt{c^4 - 4b^2c}}{2b} \quad (8)$$

The choices $b = c$, followed by $c = 1$ give the following ten matrices

$$A_1 = \begin{bmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{bmatrix}, A_2 = \begin{bmatrix} 1 & \omega & 1 \\ 1 & 1 & \omega \\ \omega & 1 & 1 \end{bmatrix}, A_3 = \begin{bmatrix} \omega & \omega & 1 \\ 1 & \omega & \omega \\ \omega & 1 & \omega \end{bmatrix}, A_4 = \begin{bmatrix} 1 & 1 & \omega \\ \omega & 1 & 1 \\ 1 & \omega & 1 \end{bmatrix}, A_5 = \begin{bmatrix} \omega & 1 & \omega \\ \omega & \omega & 1 \\ 1 & \omega & \omega \end{bmatrix} \quad (9)$$

and respectively

$$B_1 = \begin{bmatrix} \omega^2 & 1 & 1 \\ 1 & \omega^2 & 1 \\ 1 & 1 & \omega^2 \end{bmatrix}, B_2 = \begin{bmatrix} 1 & \omega^2 & 1 \\ 1 & 1 & \omega^2 \\ \omega^2 & 1 & 1 \end{bmatrix}, B_3 = \begin{bmatrix} \omega^2 & \omega^2 & 1 \\ 1 & \omega^2 & \omega^2 \\ \omega^2 & 1 & \omega^2 \end{bmatrix}, B_4 = \begin{bmatrix} 1 & 1 & \omega^2 \\ \omega^2 & 1 & 1 \\ 1 & \omega^2 & 1 \end{bmatrix}, B_5 = \begin{bmatrix} \omega^2 & 1 & \omega^2 \\ \omega^2 & \omega^2 & 1 \\ 1 & \omega^2 & \omega^2 \end{bmatrix} \quad (10)$$

All the above ten matrices are not Hadamard

4. NEW HADAMARD MATRICES

The A_1 matrix generates two complex Hadamard matrices

$$A_{11} = \begin{bmatrix} -(-1)^{1/3} & 1 & 1 \\ 1 & -(-1)^{1/3} & 1 \\ 1 & 1 & -(-1)^{1/3} \end{bmatrix}, A_{12} = \begin{bmatrix} (-1)^{2/3} & 1 & 1 \\ 1 & (-1)^{2/3} & 1 \\ 1 & 1 & (-1)^{2/3} \end{bmatrix} \quad (11)$$

and A_{11} and A_{12} lead to a MUB set as $(\mathbb{I}, A_{11}, A_{12})$. The matrices A_{11} and A_{12} , and respectively A_{12} and A_{11} generate the following two matrices

$$A_{1112} = \begin{bmatrix} (-1)^{1/6} & -\mathbf{i} & -\mathbf{i} \\ -\mathbf{i} & (-1)^{1/6} & -\mathbf{i} \\ -\mathbf{i} & -\mathbf{i} & (-1)^{1/6} \end{bmatrix}, A_{1211} = \begin{bmatrix} (-1)^{5/6} & -\mathbf{i} & -\mathbf{i} \\ -\mathbf{i} & (-1)^{5/6} & -\mathbf{i} \\ -\mathbf{i} & -\mathbf{i} & (-1)^{5/6} \end{bmatrix} \quad (12)$$

In this case the MUB is $(\mathbb{I}, A_{1112}, A_{1211})$

The A_2 matrix generates also two complex Hadamard matrices

$$A_{21} = \begin{bmatrix} 1 & -(-1)^{1/3} & 1 \\ 1 & 1 & -(-1)^{1/3} \\ -(-1)^{1/3} & 1 & 1 \end{bmatrix}, \quad A_{22} = \begin{bmatrix} 1 & (-1)^{2/3} & 1 \\ 1 & 1 & (-1)^{2/3} \\ (-1)^{2/3} & 1 & 1 \end{bmatrix} \quad (13)$$

The matrices A_{21} and A_{22} and respectively A_{22} and A_{21} generate the same matrices (12).

The A_3 matrix generates two complex Hadamard matrices

$$A_{31} = \begin{bmatrix} -(-1)^{1/3} & -(-1)^{1/3} & 1 \\ 1 & -(-1)^{1/3} & -(-1)^{1/3} \\ -(-1)^{1/3} & 1 & -(-1)^{1/3} \end{bmatrix}, \quad A_{32} = \begin{bmatrix} (-1)^{2/3} & (-1)^{2/3} & 1 \\ 1 & (-1)^{2/3} & (-1)^{2/3} \\ (-1)^{2/3} & 1 & (-1)^{2/3} \end{bmatrix} \quad (14)$$

Matrices A_{31} and A_{32} lead to the MUB set $(\mathbb{I}, A_{31}, A_{32})$. Similar to the preceding cases matrices A_{31} and A_{32} in this order, and respectively A_{32} and A_{31} generate the matrices

$$A_{3132} = \begin{bmatrix} \mathbf{i} & -(-1)^{1/6} & -(-1)^{1/6} \\ -(-1)^{1/6} & \mathbf{i} & -(-1)^{1/6} \\ -(-1)^{1/6} & -(-1)^{1/6} & \mathbf{i} \end{bmatrix}, \quad A_{3231} = \begin{bmatrix} \mathbf{i} & -(-1)^{5/6} & -(-1)^{5/6} \\ -(-1)^{5/6} & \mathbf{i} & -(-1)^{5/6} \\ -(-1)^{5/6} & -(-1)^{5/6} & \mathbf{i} \end{bmatrix} \quad (15)$$

The above matrices generate the MUB $(\mathbb{I}, A_{3132}, A_{3231})$.

The matrices A_{1112} and A_{3122} , and respectively A_{3122} and A_{1112} generate the following matrices

$$D_{11} = \begin{bmatrix} (-1)^{1/6} & (-1)^{5/6} & (-1)^{5/6} \\ (-1)^{5/6} & (-1)^{1/6} & (-1)^{5/6} \\ (-1)^{5/6} & (-1)^{5/6} & (-1)^{1/6} \end{bmatrix}, \quad D_{12} = \begin{bmatrix} (-1)^{5/6} & (-1)^{1/6} & (-1)^{1/6} \\ (-1)^{1/6} & (-1)^{5/6} & (-1)^{1/6} \\ (-1)^{1/6} & (-1)^{1/6} & (-1)^{5/6} \end{bmatrix} \quad (16)$$

Thus the MUB is given by $(\mathbb{I}, D_{11}, D_{12})$.

The A_4 matrix generates other two matrices whose form is

$$A_{41} = \begin{bmatrix} 1 & 1 & -(-1)^{1/3} \\ -(-1)^{1/3} & 1 & 1 \\ 1 & -(-1)^{1/3} & 1 \end{bmatrix}, \quad A_{42} = \begin{bmatrix} 1 & 1 & (-1)^{2/3} \\ (-1)^{2/3} & 1 & 1 \\ 1 & (-1)^{2/3} & 1 \end{bmatrix} \quad (17)$$

and the MU pair has the form $(\mathbb{I}, A_{41}, A_{42})$. The matrices A_{41} and A_{42} , and respectively A_{42} and A_{41} generate again the matrices (12).

In the next case A_5 matrix leads also to two matrices

$$A_{51} = \begin{bmatrix} -(-1)^{1/3} & 1 & -(-1)^{1/3} \\ -(-1)^{1/3} & -(-1)^{1/3} & 1 \\ 1 & -(-1)^{1/3} & -(-1)^{1/3} \end{bmatrix}, \quad A_{52} = \begin{bmatrix} (-1)^{2/3} & 1 & (-1)^{2/3} \\ (-1)^{2/3} & (-1)^{2/3} & 1 \\ 1 & (-1)^{2/3} & (-1)^{2/3} \end{bmatrix} \quad (18)$$

with the MUB pair written as $(\mathbb{I}, A_{51}, A_{52})$. The matrices generated A_{51} , and A_{52} coincide with the matrices (11).

The matrices A_{51} , A_{52} generate the following matrices

$$A_{5152} = \begin{bmatrix} \mathbf{i} & -(-1)^{1/6} & -(-1)^{1/6} \\ -(-1)^{1/6} & \mathbf{i} & -(-1)^{1/6} \\ -(-1)^{1/6} & -(-1)^{1/6} & \mathbf{i} \end{bmatrix}, \quad A_{5251} = \begin{bmatrix} \mathbf{i} & -(-1)^{5/6} & -(-1)^{5/6} \\ -(-1)^{5/6} & \mathbf{i} & -(-1)^{5/6} \\ -(-1)^{5/6} & -(-1)^{5/6} & \mathbf{i} \end{bmatrix} \quad (19)$$

and the MUB is $(\mathbb{I}, A_{5152}, A_{5251})$.

With the B_i matrices one get similar results. Thus the B_1 matrix leads to the following diagonal matrices

$$B_{11} = \begin{bmatrix} (-1)^{2/3} & 1 & 1 \\ 1 & (-1)^{2/3} & 1 \\ 1 & 1 & (-1)^{2/3} \end{bmatrix}, \quad B_{12} = \begin{bmatrix} -(-1)^{1/3} & 1 & 1 \\ 1 & -(-1)^{1/3} & 1 \\ 1 & 1 & -(-1)^{1/3} \end{bmatrix} \quad (20)$$

The MUB set is $(\mathbb{I}, B_{11}, B_{12})$. Similar to the preceding cases B_{11} and B_{12} generate the matrices (19).

The B_2 matrix leads to

$$B_{21} = \begin{bmatrix} (-1)^{2/3} & 1 & 1 \\ 1 & (-1)^{2/3} & 1 \\ 1 & 1 & (-1)^{2/3} \end{bmatrix}, \quad B_{22} = \begin{bmatrix} -(-1)^{1/3} & 1 & 1 \\ 1 & -(-1)^{1/3} & 1 \\ 1 & 1 & -(-1)^{1/3} \end{bmatrix} \quad (21)$$

and the MUB set is $(\mathbb{I}, B_{21}, B_{22})$. Matrices B_{2122} and B_{2221} coincide with the matrices A_{1112} and A_{2111} .

The B_3 matrix generates other two matrices

$$B_{31} = \begin{bmatrix} (-1)^{2/3} & (-1)^{2/3} & 1 \\ 1 & (-1)^{2/3} & (-1)^{2/3} \\ (-1)^{2/3} & 1 & (-1)^{2/3} \end{bmatrix}, \quad B_{32} = \begin{bmatrix} -(-1)^{1/3} & -(-1)^{1/3} & 1 \\ 1 & -(-1)^{1/3} & -(-1)^{1/3} \\ -(-1)^{1/3} & 1 & -(-1)^{1/3} \end{bmatrix} \quad (22)$$

The MU set is $(\mathbb{I}, B_{31}, B_{32})$. Matrices B_{31} and B_{32} generate the matrices A_{5152} and A_{5251} .

The B_4 matrix generate the following two Hadamard matrices

$$B_{41} = \begin{bmatrix} 1 & 1 & (-1)^{2/3} \\ (-1)^{2/3} & 1 & 1 \\ 1 & (-1)^{2/3} & 1 \end{bmatrix}, \quad B_{42} = \begin{bmatrix} 1 & 1 & -(-1)^{1/3} \\ -(-1)^{1/3} & 1 & 1 \\ 1 & -(-1)^{1/3} & 1 \end{bmatrix} \quad (23)$$

and the MU form is $(\mathbb{I}, B_{41}, B_{42})$. The matrices B_{41} and B_{42} generate the matrices

$$B_{4142} = \begin{bmatrix} (-1)^{5/6} & -\mathbf{i} & -\mathbf{i} \\ -\mathbf{i} & (-1)^{5/6} & -\mathbf{i} \\ -\mathbf{i} & -\mathbf{i} & (-1)^{5/6} \end{bmatrix}, \quad B_{4241} = \begin{bmatrix} (-1)^{1/6} & -\mathbf{i} & -\mathbf{i} \\ -\mathbf{i} & (-1)^{1/6} & -\mathbf{i} \\ -\mathbf{i} & -\mathbf{i} & (-1)^{1/6} \end{bmatrix} \quad (24)$$

The MUB is given by $(\mathbb{I}, B_{4142}, B_{4241})$.

As usually the B_5 matrix generates other two matrices

$$B_{51} = \begin{bmatrix} (-1)^{2/3} & 1 & (-1)^{2/3} \\ (-1)^{2/3} & (-1)^{2/3} & 1 \\ 1 & (-1)^{2/3} & (-1)^{2/3} \end{bmatrix}, \quad B_{52} = \begin{bmatrix} -(-1)^{1/3} & 1 & -(-1)^{1/3} \\ -(-1)^{1/3} & -(-1)^{1/3} & 1 \\ 1 & -(-1)^{1/3} & -(-1)^{1/3} \end{bmatrix} \quad (25)$$

The MUB pair is $(\mathbb{I}, B_{51}, B_{52})$.

The matrices A_{1112} and B_{5152} generate the unitary diagonal matrix

$$I_{2/3} = \begin{bmatrix} (-1)^{2/3} & 0 & 0 \\ 0 & (-1)^{2/3} & 0 \\ 0 & 0 & (-1)^{2/3} \end{bmatrix} \quad (26)$$

The correponding MUB have the form $(\mathbb{I}_{2/3}, A_{1112}, B_{5152})$. The same matrix is generated by A_{4142} and B_{5152} , etc.

The matrices B_{3132} and A_{1112} generate another unitary diagonal matrix

$$I_{1/3} = \begin{bmatrix} -(-1)^{1/3} & 0 & 0 \\ 0 & -(-1)^{1/3} & 0 \\ 0 & 0 & -(-1)^{1/3} \end{bmatrix} \quad (27)$$

The MUB in this case has the form $(\mathbb{I}_{m1/3}, B_{5152} A_{1112})$, where $m = -1$. The same matrix is generated by B_{5152} and A_{2122} , and respectively by B_{4122} and A_{3132} , etc.

Our approach has shown that the matrices A_i and B_i , $i = 1, 2, 3, 4, 5$ are not complex Hadamard matrices. Thus the first step was to make use of the Sylvester trick, see equation (3), in order to transform all the matrices which depend on ω and ω^2 into true Hadamard matrices. The final result is that with them we found many new MU bases.

5. THE FIVE DIMENSIONAL CASE

This case is very interesting because there is a 5-dimensional circulant matrix of the following form

$$C_5 = \begin{bmatrix} 1 & a & a^4 & a^4 & a \\ a & 1 & a & a^4 & a^4 \\ a^4 & a & 1 & a & a^4 \\ a^4 & a^4 & a & 1 & a \\ a & a^4 & a^4 & a & 1 \end{bmatrix} \quad (28)$$

which leads to new complex Hadamard matrices. For this we make use of the relation (3) for getting complex Hadamard matrices from C_5 matrix. The diagonal entries are equal to 1. The off diagonal entries contain the polynomial $1 + a + a^2 + a^3 + a^4$

For that we make use of the Sylvester relation [5], and the resulting matrix has 1 on the main diagonal and all the other entries have a common factor given by

$$1 + a + a^2 + a^3 + a^4 \quad (29)$$

The solutions of (29) give 5-dimensional matrices, and they are

$$sol = [a_1 = -1(-1)^{1/5}, a_2 = (-1)^{2/5}, a_3 = -1(-1)^{3/5}, a_4 = (-1)^{4/5}] \quad (30)$$

By using each solution in matrix (28) we get four different matrices denoted by D_i , $i = 1, 2, 3, 4$. They are

$$D_1 = \begin{bmatrix} 1 & -(-1)^{1/5} & (-1)^{4/5} & (-1)^{4/5} & -(-1)^{1/5} \\ -(-1)^{1/5} & 1 & -(-1)^{1/5} & (-1)^{4/5} & (-1)^{4/5} \\ (-1)^{4/5} & -(-1)^{1/5} & 1 & -(-1)^{1/5} & (-1)^{4/5} \\ (-1)^{4/5} & (-1)^{4/5} & -(-1)^{1/5} & 1 & -(-1)^{1/5} \\ -(-1)^{1/5} & (-1)^{4/5} & (-1)^{4/5} & -(-1)^{1/5} & 1 \end{bmatrix}, \quad D_2 = \begin{bmatrix} 1 & (-1)^{2/5} & -(-1)^{3/5} & -(-1)^{3/5} & (-1)^{2/5} \\ (-1)^{2/5} & 1 & (-1)^{2/5} & -(-1)^{3/5} & -(-1)^{3/5} \\ -(-1)^{3/5} & (-1)^{2/5} & 1 & -(-1)^{2/5} & -(-1)^{3/5} \\ -(-1)^{3/5} & -(-1)^{3/5} & (-1)^{2/5} & 1 & (-1)^{2/5} \\ (-1)^{2/5} & -(-1)^{3/5} & -(-1)^{3/5} & (-1)^{2/5} & 1 \end{bmatrix} \quad (31)$$

$$D_3 = \begin{bmatrix} 1 & -(-1)^{3/5} & (-1)^{2/5} & (-1)^{2/5} & -(-1)^{3/5} \\ -(-1)^{3/5} & 1 & -(-1)^{3/5} & (-1)^{2/5} & (-1)^{2/5} \\ (-1)^{2/5} & -(-1)^{3/5} & 1 & -(-1)^{3/5} & (-1)^{2/5} \\ (-1)^{2/5} & (-1)^{2/5} & -(-1)^{3/5} & 1 & -(-1)^{3/5} \\ -(-1)^{3/5} & (-1)^{2/5} & (-1)^{2/5} & -(-1)^{3/5} & 1 \end{bmatrix}, \quad D_4 = \begin{bmatrix} 1 & (-1)^{4/5} & -(-1)^{1/5} & -(-1)^{1/5} & (-1)^{4/5} \\ (-1)^{4/5} & 1 & (-1)^{4/5} & -(-1)^{1/5} & -(-1)^{1/5} \\ -(-1)^{1/5} & (-1)^{4/5} & 1 & (-1)^{4/5} & -(-1)^{1/5} \\ -(-1)^{1/5} & -(-1)^{1/5} & (-1)^{4/5} & 1 & (-1)^{4/5} \\ (-1)^{4/5} & -(-1)^{1/5} & -(-1)^{1/5} & (-1)^{4/5} & 1 \end{bmatrix} \quad (32)$$

All the above four matrices are complex Hadamard and they generate a MUB of the following form $(\mathbb{I}, D_1, D_2, D_3, D_4)$.

6. CONCLUSION

Our approach has shown that the matrices A_i and B_i are not complex Hadamard. So we used the necessary constraints to obtain new Hadamard matrices. In the same time we disproved the assertion that for 3- and 5-dimensional matrices they have the form of the corresponding Fourier matrices. An important result is that C_5 matrix generated four Hadamard matrices which disprove all assumptions rised in papers [1], [2] and [3].

[1] Björck G. and Fröberg R., "A faster way to count solutions of inhomogeneous systems of algebraic equations, with application to cyclic n -roots", J.Symb.Comput. **12**, 329 (1991)

- [2] Durt T. et al, *On mutually unbiased bases*, Int.J.Quant.Inf., **8**, 535 (2010)
- [3] Szöllősi F, *Construction, and parametrization of complex Hadamard matrices*, A Thesis Presented to Central European University in Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy in Mathematics and its Applications, arXiv: 1110.5590.pdf
- [4] Banica T. and L. Pittau, *Regularity questions for complex Hadamard matrices*, arXiv:1307.4712
- [5] Sylvester, J. J., *Thoughts on inverse orthogonal matrices, simultaneous sign-succession, and tessellated pavements in two or more colours, with application to Newton's rule, ornamental tile work, and the theory of numbers*, Philos. Mag. **34**, 461 (1867)